AMENDMENT TO THE SPECIFICATION

Please replace the paragraph beginning on page 2, line 1 with the following rewritten paragraph:

Paper on the DTCP specification ~~(URL: http://www.dtcp.com/spec.html)~~, while disclosure relating to challenge-response authentication, elliptic-curve DSA signatures, and elliptic-curve DH key sharing can be found in *Modern Cryptography* by Tatsuaki OKAMOTO and Hirosuke YAMAMOTO (Sangyo Tosho Publishing, 1997, available in Japanese only).

Please replace the paragraph beginning on page 2, line 8 with the following rewritten paragraph:

However, there is uncertainty in terms of the as yet unproven security of the authentication/key-sharing scheme stipulated by DTCP. Here, proof of security refers, in public key encryption, to proving that a user not in possession of a secret key is unable to decipher ciphertext, based on the assumption that the related mathematical problems are difficult to solve, and provides a guarantee of the security of public key encryption (see, for example, Mihir BELLARE, Phillip ROGAWAY, "Minimizing the use of random oracles in authenticated encryption schemes", 1997 ~~(URL: http://www.cs.ucdavis.edu/research/tech-reports/1997/CSE-97-8.pdf)~~.

Please replace the paragraph beginning on page 23, line 5 with the following rewritten paragraph:

PSEC-KEM is described here as an exemplary key encapsulation mechanism. Note that detailed disclosure relating to PSEC-KEM can be found in Tatsuaki OKAMOTO, "Generic conversions for constructing IND-CCA2 public-key encryption in the random oracle model" (5th Workshop on Elliptic Curve Cryptography, ECC 2001, 30 October 2001~~, URL:http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/okamoto.ppt, viewed: September 29, 2002)~~.